HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 200207938-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	**Sundaresan Ramamoorthy, et al.**	**Confirmation No.:**	**6770**
Application No.:	**10/690,605**	**Examiner:**	**Hoang, Daniel L.**
Filing Date:	**October 23, 2003**	**Group Art Unit:**	**2136**

Title: SMART TRANSLATION OF GENERIC CONFIGURATION

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on August 13, 2007.

☒ The fee for filing this Appeal Brief is $510.00 (37 CFR 41.20).

☐ No Additional Fee Required.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

☐ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

☒	1st Month $120	☐	2nd Month $460	☐	3rd Month $1050	☐	4th Month $1640

☐ The extension fee has already been filed in this application.

☐ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of $ 630. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees.

☐ A duplicate copy of this transmittal letter is enclosed.

☐ I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:
Commissioner for Patents, Alexandria, VA 22313-1450
Date of Deposit:

OR

☐ I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (571)273-8300.
Date of facsimile:
Typed Name:
Signature:_____

Respectfully submitted,
Sundaresan Ramamoorthy, et al.
By:_____
Sean S. Wooden
Attorney/Agent for Applicant(s)
Reg No. : 43,997
Date : November 13, 2007
Telephone : (202) 662-2700

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.	:	10/690,605
Applicant	:	Sundaresan Ramamoorthy, et al.
Filed	:	October 23, 2003
Title	:	SMART TRANSLATION OF GENERIC CONFIGURATION
TC/A.U.	:	2136
Examiner	:	Hoang, Daniel L.
Docket No.	:	200207938-1
Customer No.	:	022879

Mail Stop Appeal Brief - Patents
Commissioner of Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPEAL BRIEF UNDER 37 C.F.R. §41.37

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

Hewlett Packard Company is the real party in interest.

II. RELATED APPEALS AND INTERFERENCES

There are no other related appeals or interferences.

III. STATUS OF CLAIMS

Claims 1-18 are pending in the application. Claims 1-18 stand rejected. Applicants appeal the rejection of claims 1-18.

IV. STATUS OF AMENDMENTS

There were no amendments filed after final.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Appellants have discovered a new, improved system, method and computer readable medium for implementing a policy in a network. The prior art does not describe, teach or suggest a system as in claim 1. Appellants' system includes a plurality of device-agnostic policy implementations, in which the device-agnostic policy implementations 120 include non-security policy implementations, a plurality of network devices 140, at least two of said devices being dissimilar, and a plurality of device translators 130, each device translator corresponding to a respective one of said plurality of network devices and one of said plurality of device-agnostic policy implementations, at least two of said device translators being dissimilar, each of said plurality of device translators translating said device-agnostic policy implementation into corresponding device-specific implementations (*e.g.*, p. 4, lines 7-23 and p. 5, line 1 through p. 7, line 26, FIG. 1).

The prior art also does not describe, teach or suggest a method as in claim 10. Appellants' method represents 205 a vendor-agnostic configuration, builds 210 a translator for a specific policy and vendor, in which the computer network includes a plurality of policies and vendors, the policies including non-security policies, repeats the building for each type of policy and vendor, identifies 215 a device, loads 220 said translator, and translates 225 said vendor-agnostic configuration into vendor-specific configuration using said translator and repeats the identifying, loading and translating for each type of policy and vendor (*e.g.*, p. 4, lines 24-29 and p. 5, line 1 through p. 7, line 26, FIG. 2).

Moreover, the prior art does not describe, teach or suggest a computer readable medium as in claim 18. Appellants' computer readable medium contains instructions for implementing a policy in a computer network. The instructions include instructions that represent 205 a vendor-agnostic configuration, build 210 a translator for a specific policy and vendor, in which the computer network includes a plurality of policies and vendors, the policies including non-security policies, repeat the building for each type of policy and vendor, identify 215 a device, loads 220 said translator, and translate 225 said vendor-agnostic configuration into vendor-specific configuration using said translator and repeat the identifying, loading and translating for each type of policy and vendor (*e.g.*, p. 4, lines 24-29 and p. 5, line 1 through p. 7, line 26, FIG. 2).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

(1) Claims 1-8, 10-16 and 18 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Pre-Grant Publication No. 20040193912 to Li et al. ("Li") (See May 11, 2007 Office Action (the "Office Action"), p. 3, para. 3); and

(2) Claims 9 and 17 stand rejected under 35 U.S.C. § 103(a) as being obvious over Li in view of U.S. Pre-grant publication No. 20050160361 to Young ("Young") (See Office Action, p. 6, para. 1).

VII. ARGUMENT

The pending claims are patentable over the cited prior art. As noted above, the Office Action sets forth two grounds for rejection, one under 35 U.S.C. § 102 and the other under 35 U.S.C. § 103. Central to each of these grounds of rejection is the Li reference. The rejections set forth by the Examiner must fail because Li fails to describe each and every limitation of the independent claims. The additional cited prior art Young fails to overcome these defects in Li. Since the prior art references fail to teach or suggest all of the claim limitations, the Final Office Action fails to establish a *prima facie* case of anticipation or obviousness and the claims must be allowed.

A. Li Fails to Expressly or Inherently Describe A Plurality Of Device-Agnostic Policy Implementations, In Which The Device-Agnostic Policy Implementations Include Non-Security Policy Implementations

Claims 1-8, 10-16 and 18 are rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Pre-Grant Publication No. 20040193912 to Li et al. ("Li"). However, to anticipate a claim, each and every element as set forth in the claim must be found, either expressly or inherently described, in a single prior art reference. Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987); see also MPEP § 2131. Moreover, the "identical invention must be shown in as complete detail as is contained in the ... claim." Richardson v. Suzuki Motor Co., 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

Li does not expressly or inherently describe each and every of claims 1-8 and 10-16. Specifically, Li does not expressly or inherently describe "a plurality of device-agnostic policy implementations, in which the device-agnostic policy implementations include non-security policy implementations," as recited in independent claim 1. For the same reasons, Li does not expressly or inherently describe "building a translator for a specific policy and vendor...the policies including non-security policies," as recited in claims 10 and 18.

The Examiner does not specifically cite anything to teach this element in his rejection Indeed, this is not surprising since Li is limited to security policies. Rather, the Examiner only addresses this element in his response to arguments. There, the Examiner sites to paragraph 30 of the Li reference as teaching an application module capable of monitoring and tracking security threat information or event information. Examiner interprets the tracking of event information to be equivalent to backup, *i.e.*, a non-security policy implementation. As is shown below, Li teaches tracking of security event information, not merely event information. Furthermore, tracking security event information is not equivalent to backup. Finally, even if Li taught backing-up, it is specifically limited to security policies and does

not teach non-security policy implementations. Therefore, neither this paragraph nor any other part of Li describes this element.

1. Li Teaches Tracking Security Event Information

As noted above, the Examiner cites paragraph 30 of Li as showing that Li teaches a non-security implementation. Specifically, the Examiner argues that Li's teaching of an application module capable of monitoring and tracking security threat information or event information shows that Li teaches backing up, a non-security implementation. However, a brief review of Li and the context of this statement show that Li is discussing tracking security event information, not mere event information. Paragraph 30 is describing a portion of Figure 2, which is a "flow diagram of a method for managing security policies." More specifically, paragraph 30 and the above statement describe that "a Policy Feedback Point (PFP) module monitors and tracks, at 230, the security threat information or event information." The referenced block 230 in Figure 2 makes clear that the event information is security event information, as it is labeled "Monitor and/or Track *Security* Transactions." [Emphasis added]. Moreover, the additional text describing the PFP module and Figure 2 makes clear that Li is *only* discussing security policies, specifically analyzing the security threat and element information to dynamically adjust security policies, as depicted at 252. See, *e.g.*, paragraphs [0031]-[0036] and Figure 2. In this context, the only possible conclusion is that Li is monitoring and tracking security information. Consequently, the cited paragraph 30 does not show that Li teaches a non-security implementation.

2. Tracking Security Event Information Is Not Equivalent To Backing Up

Regardless of whether the event information was security event information or not, tracking and monitoring event information is not equivalent to backing-up, as the Examiner asserts. Backing-up means making a copy of an original file and storing it separately from the original. See Webster's II New College Dictionary. Tracking and monitoring event information is clearly not backing-up. Moreover, an examination of Figure 2 shows that the event information is used to dynamically adjust *security policies* 252. See paragraph [0032] and Figure 2 [Emphasis added]. Clearly then, tracking event information as taught by Li is part of a *security policy* implementation, not a non-security policy implementation.

3. Li Only Describes Security Policy Implementations

The title of Li is very telling: "Methods and Systems for Managing *Security Policies*." [Emphasis added]. This title, and indeed the entire specification show that Li is only

concerned with security policies and security policy implementations. The technical field of Li states that "[e]mbodiments of the present invention related generally to automated security management, and more particularly to providing automated management for security policies." In this context, every action or application that Li describes or mentions is directed towards a security policy implementation. The Appellants' claimed invention, however, is not so limited. As is made clear in the by the following, Appellants' claimed invention is significantly broader: [f]or the purposes of illustration, only access control 112 is used to describe the present invention, although it should be understood that the present invention may be applied to all of the policy definitions 110, as well as other policy definitions." See p. 4, lines 10-13. Consequently, Li cannot describe, inherently or explicitly, a plurality of device-agnostic policy implementations, in which the device-agnostic policy implementations include non-security policy implementations. Therefore, Li does not anticipate claims 1-8, 10-16 or 18 and Appellants respectfully request the withdrawal of this rejection.

B. Li Does Not Teach A Plurality of Device Translators, Each Device Translator Corresponding To One of Said Network Devices and One of Said Device-Agnostic Implementations

Li also fails to expressly or inherently describe "a plurality of device translators, each device translator corresponding to one of said network devices and one of said device-agnostic implementations," as recited in claim 1. Likewise, Li fails to expressly or inherently describe "building a translator for a specific policy and vendor," as recited in claims 10 and 18. The Examiner does not cite any section of Li as describing a plurality of device translators each corresponding to one of said network devices and one of said device-agnostic implementations. Rather, Examiner relies on previous citation to paragraph [0028]. However, paragraph [0028] merely shows that Li describes "one or more policy decision translators." It states that these translators "acquire, distribute, or push security policies to the appropriate security-enabled devices over the network." Nothing in this sentence suggests that each translator corresponds to one network device, let alone one device-agnostic implementation. Indeed, the following sentence suggests the opposite: "[t]he policy decision translators include logic to convert the intermediate data format of the security policies to needed data formats that can be used by each of the security-enabled devices." [Emphasis added]. The underlined text shows the translators translating for multiple devices (formats for each of the security-enabled devices) and for multiple policies (format of the security policies). Therefore, Li not only fails to inherently or expressly describe a plurality of device translators each corresponding to one of said network devices and one of said device-agnostic

implementations, but Li explicitly describes the opposite, translators corresponding to multiple implementations and multiple devices. Consequently, Li fails to anticipate claims 1-8, 10-16 or 18 and Appellants respectfully request the withdrawal of this rejection.

C. Young Combined With Li Fails To Render The Claims Obvious

Claims 9 and 17 are rejected under 35 U.S.C. § 103(a) as being obvious over Li in view of Young. Young was cited merely as teaching Java. Young, therefore, does not cure the above defects of Li described above. Consequently, claims 9 and 17 are allowable for the same reasons as described above. Consequently, claims 9 and 17 are not rendered obvious and Appellants respectfully request the withdrawal of this rejection.

The appeal brief fee in the amount of **$510.00** along with an extension fee for one month in the amount of **$120.00** is being paid on the accompanying transmittal letter for an appeal brief. Should there be any additional fees required for this appeal brief, please charge any fees required or credit any over payment to **Deposit Account 08-2025** pursuant to 37 CFR 1.25.

Respectfully submitted,

Date: **November 13, 2007**

Sean S. Wooden, Reg. No. 43,997
ANDREWS KURTH LLP
1350 I Street, NW
Suite 1100
Washington, D.C. 20005
Telephone: (202) 662-3051
Fax: (202) 662-2739

CLAIMS APPENDIX

Claim 1 (previously presented): A system for implementing a policy in a network, said system comprising:

a plurality of device-agnostic policy implementations, in which the device-agnostic policy implementations include non-security policy implementations;

a plurality of network devices, at least two of said devices being dissimilar; and

a plurality of device translators, each device translator corresponding to a respective one of said plurality of network devices and one of said plurality of device-agnostic policy implementations, at least two of said device translators being dissimilar, each of said plurality of device translators translating said device-agnostic policy implementation into corresponding device-specific implementations.

Claim 2 (original): The system according to claim 1, wherein said device-agnostic policy implementation is selected from the group consisting of firewall, Virtual Private Network, Java 2 Enterprise Edition Application, and custom operating system.

Claim 3 (original): The system according to claim 1, wherein said device-agnostic policy implementation implements a policy selected from the group consisting of access control, quality of service, backup, and availability.

Claim 4 (original): The system according to claim 1, wherein said device translators are represented by Extensible Stylesheet Language (XSL) code.

Claim 5 (original): The system according to claim 1, wherein said device-agnostic policy implementation is Extensible Markup Language (XML) code.

Claim 6 (original): The system according to claim 3, wherein said policy is represented by Extensible Markup Language (XML) code.

Claim 7 (original): The system according to claim 1, wherein the device-specific implementation is represented by Command Line Interface (CLI) code.

Claim 8 (original): The system according to claim 1, wherein the device-specific implementation is represented by Application Programming Interface (API) code.

Claim 9 (original): The system according to claim 1, wherein the device-specific implementation is represented by Java code.

Claim 10 (previously presented): A method comprising:

representing a vendor-agnostic configuration;

building a translator for a specific policy and vendor, in which the computer network includes a plurality of policies and vendors, the policies including non-security policies;

repeating the building for each type of policy and vendor;

identifying a device;

loading said translator;

translating said vendor-agnostic configuration into vendor-specific configuration using said translator; and

repeating the identifying, loading and translating for each type of policy and vendor.

Claim 11 (original): The method according to claim 10, wherein said vendor-agnostic configuration is represented by Extensible Markup Language (XML) code.

Claim 12 (original): The method according to claim 10, wherein said translator is represented by Extensible Stylesheet Language (XSL) code.

Claim 13 (original): The system according to claim 10, wherein said specific policy is selected from the group consisting of firewall, Virtual Private Network, Java 2 Enterprise Edition Application, and custom operating system.

Claim 14 (original): The system according to claim 10, wherein said specific policy is selected from the group consisting of access control, quality of service, backup, and availability.

Claim 15 (original): The system according to claim 10, wherein the vendor-specific configuration is represented by Command Line Interface (CLI) code.

Claim 16 (original): The system according to claim 10, wherein the vendor-specific configuration is represented by Application Programming Interface (API) code.

Claim 17 (original): The system according to claim 10, wherein the vendor-specific configuration is represented by Java code.

Claim 18 (previously presented): A computer readable medium containing instructions for implementing a policy in a computer network, said instructions comprising:

representing a vendor-agnostic configuration;

building a translator for a specific policy and vendor, in which the computer network includes a plurality of policies and vendors, the policies including non-security policies;

repeating the building for each type of policy and vendor;

identifying a device;

loading said translator;

translating said vendor-agnostic configuration into vendor-specific configuration using said translator; and

repeating the identifying, loading and translating for each type of policy and vendor.

EVIDENCE APPENDIX

No evidence submitted.

RELATED PROCEEDINGS APPENDIX

No related proceedings.